VISA

A Test of Resilience:

Fraud, Cyber Risk, and the Power of Collaboration Across CEMEA

© 2026 Visa. All rights reserved.

Point of View

A Test of Resilience: Fraud, Cyber Risk, and the Power of Collaboration Across CEMEA

Charles Lobo
Regional Risk Officer, Visa Central and Eastern Europe, Middle East, and Africa (CEMEA)

Foreword

The recent conflict involving the US, Israel, and Iran has introduced a new layer of volatility into an already complex operating environment. Its implications extend beyond Central and Eastern Europe, Middle East, and Africa (CEMEA) and into a wider global economy. The IMF notes that about 25% to 30% of global oil and 20% of liquefied natural gas pass through the Strait of Hormuz, underscoring how disruption in the region can quickly ripple through energy markets, trade flows, and financial conditions worldwide.[3]

For businesses, financial institutions, and the payments ecosystem, this is not simply a geopolitical backdrop. It is an active operating context that influences customer behavior, business continuity, and the speed at which risk conditions can change.

For payments leaders, this matters in practical ways. Periods of uncertainty do not usually create entirely new categories of fraud and cyber risk. More often, they intensify familiar threats, accelerate their pace, and reduce the time available to interpret and respond. With Artificial Intelligence reshaping both attack and defense in parallel, the agility requirements have been raised even for the most mature risk teams.

In the current times, it is clear: resilience depends on disciplined execution, timely visibility, and strong collaboration across the ecosystem. This paper sets out that view and considers what it means for institutions working across CEMEA today.

© 2026 Visa. All rights reserved.

Executive summary

Central and Eastern Europe, Middle East, and Africa (CEMEA) is operating through a period of sustained uncertainty shaped by the current conflict in the Middle East, broader regional spillover effects, and a more volatile economic and operating environment. In this setting, fraud and cyber risk are becoming more dynamic, more event-driven, and more closely connected to external developments.

From Visa's perspective, the core shift is not that the fraud landscape has become unrecognizable. It is that familiar threats are surfacing faster, evolving more quickly, and appearing less evenly across channels, customer segments, and use cases. Fraud spikes are increasingly linked to external events such as geopolitical developments, crisis communications, public announcements, or periods of visible disruption. Threat actors move quickly to exploit urgency, fear, distraction, and operational strain.

This is unfolding at a time when AI is changing the economics of both attack and defense. Threat actors are using AI to improve realism, precision, and scale of phishing, impersonation, and identity-based fraud. At the same time, AI is becoming increasingly central to detection, decisioning, and pattern recognition across the payments ecosystem.

The implication is straightforward: strong controls, monitoring, escalation, and collaboration remain essential, but they must now be applied more dynamically, with faster feedback loops and more precise calibration.

Visa helps clients improve through visibility, intelligence, modernized infrastructure, AI-enabled defenses, and close ecosystem collaboration. In uncertain times, resilience depends not only on prevention, but on the ability to detect earlier, adapt faster, and act together.

Key Takeaways

- The current conflict in the Middle East is contributing to a more volatile operating environment for businesses, institutions, and consumers.
- Periods of uncertainty tend to intensify familiar fraud and cyber patterns rather than create entirely new ones.
- AI is strengthening both attack and defense, making agility a requirement even for mature risk teams.
- Fraud resilience and operational resilience are becoming more tightly connected.
- The most effective response is vigilance without overreaction: better monitoring, faster interpretation, more precise controls, and quicker enterprise wide collaboration.

1. Why This Moment Matters

The recent Middle East conflict has introduced a new layer of volatility into an already complex operating environment. International institutions have highlighted the spillover effects across energy, trade, logistics, and financial conditions. For institutions across CEMEA, this means operating in conditions where customer behavior, business processes, and market signals may shift more quickly and less predictably.[3][4][5]

For the payments ecosystem, the risk implication is not simply that fraud rises in a linear way during crisis. More often, uncertainty changes the tempo, distribution, and detectability of risk. Established attack patterns become more adaptive and more difficult to identify early. Legitimate behavior becomes harder to distinguish from suspicious behavior. And the time available to identify, assess, and contain emerging threats often narrows.

This is particularly relevant in CEMEA, where geopolitical instability can act not only as a backdrop to risk, but as an operational trigger. Threat actors use moments of disruption to exploit heightened public anxiety, emergency communications, service interruptions, and attention gaps. In this sense, periods of conflict do not just elevate risk; they can also accelerate it.

© 2026 Visa. All rights reserved.

2. A More Event-Driven Fraud Landscape

The current CEMEA fraud landscape is increasingly event-driven rather than cyclical. Fraud activity is less likely to build gradually and more likely to spike quickly in response to external developments. Public announcements, geopolitical developments, crisis-related messaging, and operational disruption can all act as triggers.

These surges are often fast, coordinated, and multi-vector. They can affect customer-facing channels, digital account access, payment credentials, and broader trust in the ecosystem at the same time. This makes static risk assumptions less reliable. It also means that risk teams need to think less in terms of average exposure and more in terms of rapid, localized pressure.

The regional threat environment also reflects overlapping activity from different types of actors:

- Nation-state-aligned bad actors may seek disruption, data corruption, or erosion of trust in financial infrastructure.
- Hacktivist groups may prioritize visibility and reputational impact through denial-of-service attacks, defacement, or leaks.
- Financially motivated criminals remain highly opportunistic and often move fastest to convert crisis narratives into credential theft, payment data capture, and account takeover.

These actors may differ in intent, but they can converge around the same moments of instability. That is why the effect on institutions can be broader than direct financial loss alone. In this environment, disruption itself can become part of the threat.

© 2026 Visa. All rights reserved.

3. Familiar Threats, Sharpened by Current Conditions

The most common threat patterns in uncertain periods remain recognizable, but they become more persuasive and more difficult to manage.

One recurring pattern is impersonation. Fraudsters mimic trusted entities such as government bodies, law enforcement, emergency services, or crisis-management organizations to obtain personal or financial information. These schemes can arrive through voice calls, SMS, fake websites, or spoofed mobile interfaces.

A second pattern is crisis-themed phishing, in which urgent messaging is used to prompt immediate action. Messages may reference emergency payments, compensation, aid, or relief to persuade individuals to share credentials, payment details, or one-time passcodes.

A third pattern is malware-enabled payment data capture, often linked to fake news, donation appeals, charity schemes, or cryptocurrency-related lures. In such cases, malware installation may be the immediate objective, but the downstream effect is often broader credential theft and account compromise.

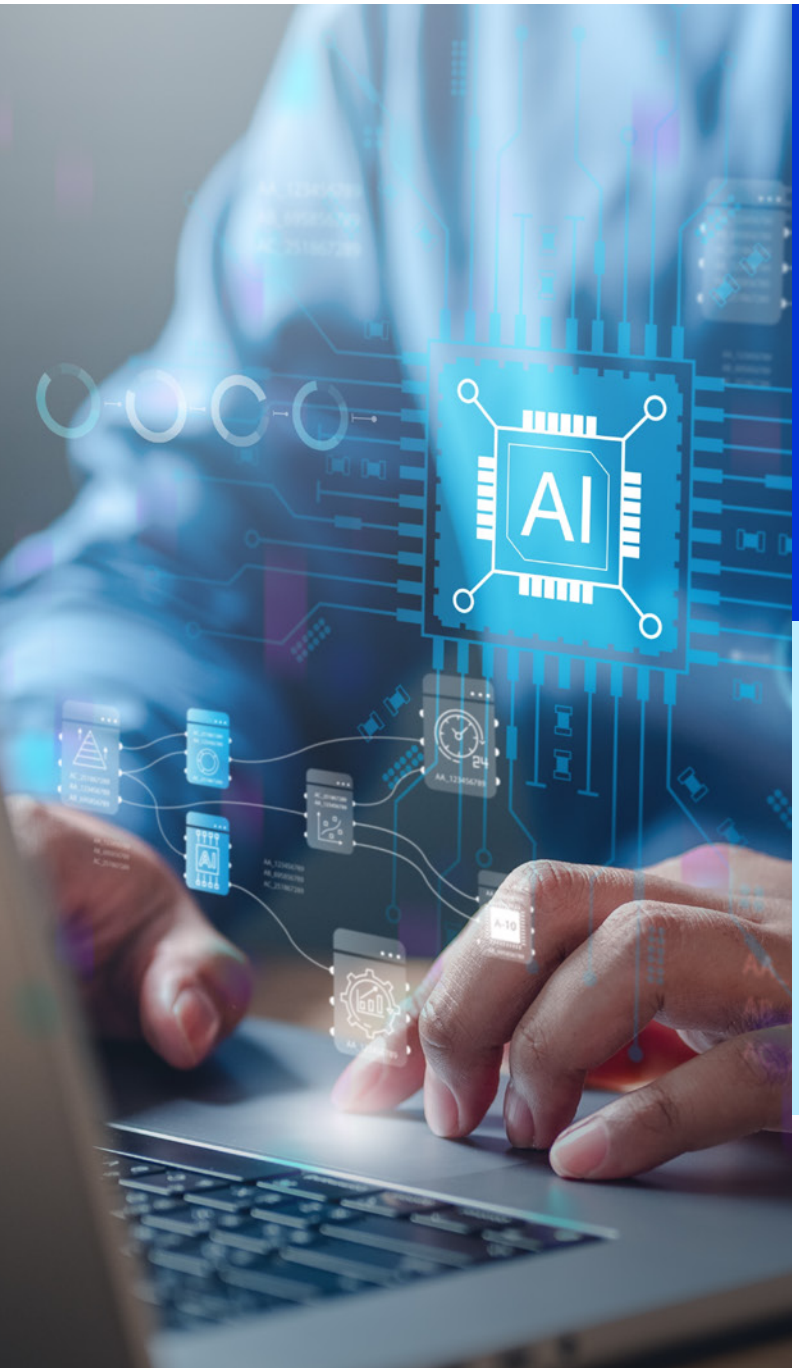
Recent warnings in the UAE illustrate how these familiar tactics continue to surface in current conditions, including scam calls using impersonation and cyber risks affecting unsecured home routers and home networks.[7][8] The broader lesson is that uncertainty does not need to create entirely new threats to create real exposure. It simply needs to make existing threats more timely, more credible, and harder to ignore.

© 2026 Visa. All rights reserved.

4. AI Is Raising the Bar for Everyone

One of the defining factors making today's environment more demanding is the rapid spread of AI. Visa's public security outlook has highlighted the acceleration of AI-powered identity attacks, the growing speed of criminal adaptation, and the need for faster, more adaptive defense.[1] AI is acting as a force multiplier for threat actors by improving the realism of phishing, enabling more convincing impersonation, increasing targeting precision, and accelerating campaign deployment.

In practical terms, this reduces the effectiveness of detection approaches that rely too heavily on static patterns or historical baselines. Attackers can assess, refine, and scale much more quickly than before.



At the same time, AI is also strengthening defense. It is increasingly central to anomaly detection, pattern recognition, real-time scoring, and the ability to connect weak signals across complex transaction environments. Visa has publicly pointed to these AI-enabled fraud defenses as an important part of strengthening ecosystem protection and improving detection at scale.[1][2]

This is why traditional assumptions are no longer enough. The fundamentals of risk management still matter, but AI is raising the bar, making it imperative for even mature teams to operate with greater agility.

© 2026 Visa. All rights reserved.

5. The Right Response: Vigilance Without Overreaction

In uncertain periods, one of the most important disciplines is calibrated response. The instinct to tighten controls broadly is understandable, particularly when threat levels are rising quickly. But blunt defensive action can create its own costs, including false positives, unnecessary declines, customer friction, and disruption to legitimate commerce. In payments, resilience depends on preserving trusted activity as well as preventing bad activity.

That is why the most effective posture is disciplined vigilance rather than overreaction. Institutions should increase monitoring, review signals more frequently, and shorten escalation timelines. But they should also remain precise, distinguishing meaningful shifts from temporary noise and targeting interventions where exposure is emerging. For institutions in CEMEA, the implication is broader than fraud prevention alone. Fraud resilience and operational resilience are increasingly interconnected. Detection speed, response speed, and communication speed are now as important as prevention itself, especially when fraud surges are triggered by fast-moving external events.

In practical terms, this means:

- reassessing whether historical baselines still hold;
- connecting fraud and cyber signals more closely;
- updating thresholds and rules more dynamically;
- strengthening customer communication readiness; and
- preparing for surge-based response when external conditions shift abruptly.

© 2026 Visa. All rights reserved.

6. Visa's Role in Supporting Clients

Visa remains committed to helping clients see earlier, decide faster, and respond more precisely. As conditions across the region remain volatile, Visa is actively monitoring the threat landscape, sharing insight on emerging fraud and cyber patterns, and engaging closely with clients as risk conditions evolve.

Visa is continuing to strengthen the capabilities that matter most in periods of uncertainty. As attacks become more adaptive and increasingly identity-led, Visa is investing in intelligence, infrastructure, and AI-enabled defenses to help clients detect threats earlier, calibrate controls more effectively, and respond with greater speed and confidence.

At the same time, Visa is working closely across the ecosystem — with clients, merchants, processors, and public-sector partners — to share signals, validate emerging risks, and support a more coordinated and resilient response. This includes helping clients interpret fast-changing developments, reassess assumptions where needed, and respond in a way that protects both security and legitimate commerce.

Visa is also deepening client engagement through awareness sessions and webinars, helping institutions stay informed on relevant trends, fraud patterns, and practical response considerations in the current environment. In uncertain periods, this combination of monitoring, capability, and partnership is essential to maintaining trust and strengthening resilience across the payments ecosystem.

© 2026 Visa. All rights reserved.

7. Collaboration as an Operational Advantage

No institution sees the full risk picture on its own. Issuers, acquirers, merchants, processors, fintechs, and networks each hold part of the signal. In stable periods, those fragments may be easier to interpret independently. In uncertain periods, they become significantly more valuable when combined.

But collaboration cannot be limited to the external ecosystem alone. It also needs to operate at the enterprise level within institutions themselves. Fraud, cyber, operations, customer communications, and incident response cannot function as isolated workstreams when threat conditions are shifting quickly. Effective resilience depends on ensuring that prevention, mitigation, and remediation are aligned and working together, so that institutions can identify risk earlier, contain it faster, and recover more effectively.

This is why collaboration matters most when signals are incomplete. Once a threat pattern is fully obvious, response becomes reactive. The greater advantage comes earlier, when institutions are still pressure-testing assumptions, identifying weak signals, and deciding whether a pattern is isolated or systemic.

In some CEMEA markets shaped by active conflict, event-driven fraud, and faster cyber-fraud convergence, close collaboration is not a secondary consideration. It is an operational capability. It supports earlier detection, better calibration, and more resilient response across the ecosystem.

© 2026 Visa. All rights reserved.

Conclusion

Given the changes in geopolitical stability, for payments leaders, the key lesson is not that the fundamentals of risk management have changed entirely. It is that familiar risks are moving faster, appearing less evenly, and becoming harder to manage through static assumptions alone.[3][4][5]

At the same time, AI is reshaping both attack and defense. That makes this a moment not for overreaction, but for sharper execution: stronger monitoring, faster interpretation, more agile controls, and closer collaboration.[1][2]

Visa's perspective is clear: resilience in uncertain times depends on disciplined vigilance, modernized capability, and ecosystem partnership. That is how institutions protect trust, support legitimate commerce, and respond with confidence when conditions are under pressure.

Visa will continue to support clients with timely insights, practical guidance, and deeper engagement in the months ahead.

© 2026 Visa. All rights reserved.

Endnotes

[1] Paul Fabara, **"6 Security Trends Shaping the Payments Ecosystem in 2026,"** Visa Perspectives, January 21, 2026. https://corporate.visa.com/en/sites/visa-perspectives/security-trust/6-security-trends-shaping-the-payments-ecosystem.html

[2] **"Visa's AI-Powered Fraud Defense Delivers Record Protection,"** Visa Newsroom. https://corporate.visa.com/en/sites/visa-perspectives/newsroom/visas-ai-powered-fraud-defense-delivers-record-protection.html

[3] **"How the War in the Middle East Is Affecting Energy, Trade, and Finance,"** International Monetary Fund (IMF), March 30, 2026. https://www.imf.org/en/blogs/articles/2026/03/30/how-the-war-in-the-middle-east-is-affecting-energy-trade-and-finance

[4] **"Joint Statement by the Heads of the IEA, IMF, and World Bank Group,"** International Monetary Fund (IMF), April 1, 2026. https://www.imf.org/en/news/articles/2026/04/01/pr-26100-joint-statement-by-the-heads-of-the-iea-imf-and-wb-group

[5] **"Statement on the Conflict in the Middle East,"** World Bank Group, March 26, 2026. https://www.worldbank.org/en/news/statement/2026/03/26/world-bank-group-statement-on-the-conflict-in-the-middle-east

[6] **"MoI, Dubai Police and Visa Launch Nationwide Campaign to Combat Fraud and E-Crimes,"** UAE Ministry of Interior. https://moi.gov.ae/en/media.center/news/090825n01.aspx

[7] **"UAE Cybersecurity Council Warns Remote Work Drives Cybersecurity Risks,"** WAM / UAE Cybersecurity Council. https://www.wam.ae/en/article/bzbytjt-uae-cybersecurity-council-warns-remote-work-drives

[8] **"Beware of Scam Calls, UAE Interior Ministry Warns,"** Gulf News. https://gulfnews.com/uae/government/beware-of-scam-calls-uae-interior-ministry-warns-1.500459583

Contributors

Aastha Sharma, Omar Abuhanoud, and Savi Sachdeva.

© 2026 Visa. All rights reserved.